CERTInext

POWERED BY EMUDHRA

RESEARCH BRIEF · BLACK HAT USA 2026 EDITION

# THE NHI BLIND SPOT

Why non-human identities have become the fastest-growing, least-governed attack surface in the enterprise.

A data-led briefing for CISOs, security architects, and identity teams. Advocating end-to-end trust for every identity — human and non-human.

PQC READY · CERTIFICATE AUTHORITY · LIFECYCLE MANAGEMENT · NON-HUMAN IDENTITIES

www.certinext.io

EXECUTIVE SUMMARY

# The identities running your enterprise aren't people.

For two decades, identity security was built around people — employees, contractors, and administrators who log in, authenticate, and leave an audit trail. That world no longer reflects reality. The identities that now run the enterprise are overwhelmingly non-human: service accounts, API keys, tokens, TLS and code-signing certificates, workload identities, and, increasingly, autonomous AI agents that act on their own.

These **non-human identities (NHIs)** already outnumber human identities by orders of magnitude, they are growing far faster than any team can track manually, and they are governed by a fraction of the controls we apply to people. That gap is the **NHI blind spot**, and attackers have noticed.

This briefing sets out what the data shows and what to do about it:

- → **The scale of the problem**: how far machine identities now outnumber humans, and how fast AI agents are accelerating the curve.
- → **Why the blind spot is dangerous**: the breaches, secrets sprawl, and visibility gaps already tied to unmanaged NHIs.
- → **The clock you can't reset**: the post-quantum migration, and the crypto-agility every non-human identity needs to survive it.
- → **A practical control checklist**: the steps that close the gap, from discovery to crypto-agility.

> The through-line is simple. **You cannot secure what you cannot see**, and most organizations cannot see their non-human identities. Closing that gap is now a board-level priority, and the foundation of modern digital trust.

## 01 The identity explosion nobody planned for

The ratio of machine identities to human identities has moved from a curiosity to a governance emergency. Different studies measure different environments, but they all point the same direction: sharply up.

**109:1**

Machine identities per human (2026), up from 82:1 a year earlier

**50%**

of organizations had a breach or incident tied to a compromised machine identity

**79/109**

of those machine identities are now AI agents

CyberArk's 2025 research put the ratio at roughly 82 machine identities for every human. Palo Alto Networks' 2026 Identity Security Landscape found it had already climbed to **109:1**, a 33% jump in a single year, with 79 of those 109 now being AI agents. Independent research has separately measured NHI growth of around 44% between 2024 and 2025.

**Agentic AI is the accelerant.** Unlike a static service account or API key, an AI agent decides at runtime, chains tool calls, and can be steered by prompt injection. Gartner projects that 40% of enterprise applications will embed task-specific AI agents by the end of 2026, up from under 5% in 2025. Each of those agents needs an identity, credentials, and access, and each one is created faster than governance processes can keep up.

For a typical 500-person company, an 82:1 ratio already implies more than **40,000 non-human identities** to discover, monitor, and protect. Most organizations cannot produce an accurate inventory of even a fraction of them.

## 02 Why the blind spot is dangerous

An identity you don't know about is an identity you can't rotate, revoke, or monitor. That is precisely why NHIs have become such a productive target.

### 2.1 Breaches are already happening

In CyberArk's 2025 research, half of organizations reported a security incident or breach tied to a compromised machine identity. Several of the most public supply-chain and cloud incidents of the past two years traced back to leaked tokens, over-privileged service accounts, or mismanaged certificates rather than a compromised human login.

### 2.2 Secrets are leaking at scale

The credentials that authenticate NHIs, such as API keys, tokens, and secrets, are routinely exposed. GitGuardian's 2025 State of Secrets Sprawl report detected more than **23 million new secrets** leaked in public GitHub repositories in a single year, up sharply on the year before. Every leaked secret is a non-human credential an attacker can use without ever touching a password prompt or MFA challenge.

### 2.3 Visibility and governance are missing

The controls we take for granted for human identities, such as onboarding, least privilege, periodic review, and offboarding, are largely absent for NHIs. In one 2026 study of enterprise security leaders, 92% said they lacked full visibility into their AI identities, 86% did not enforce access policies for them, and while 71% reported that AI systems could reach core platforms such as ERP, CRM, and financial systems, only **16%** felt they governed that access effectively. Separately, 68% of organizations said they lacked identity security controls for AI altogether.

KPMG's 2026 cybersecurity report now names non-human identities a critical priority for CISOs, and Gartner's top trends for the year highlight both agentic-AI oversight and IAM's adaptation to AI agents as forces redefining cyber risk.

## 03 The clock you can't reset: post-quantum

Even organizations that treat NHI governance as tomorrow's problem face one external deadline that manual processes cannot meet: the migration to post-quantum cryptography. And unlike a human workforce, the non-human estate that has to make that migration is growing by the minute.

| DEADLINE | WHAT CHANGES | WHY IT FORCES CRYPTO-AGILITY |
|---|---|---|
| **2024** | NIST finalizes post-quantum standards (FIPS 203, 204, 205) | The algorithms to migrate to now exist; the countdown starts |
| **2027** | NSA CNSA 2.0 requires quantum-resistant crypto for new national-security acquisitions | PQC becomes a procurement gate, not a research topic |
| **2030** | NIST deprecates 112-bit algorithms (RSA-2048, P-256) | Estates must know where every key and algorithm lives |
| **2035** | NIST disallows all quantum-vulnerable public-key algorithms | Full crypto-agility and PQC migration required |

NIST finalized its post-quantum standards (FIPS 203, 204, and 205) in 2024 and set deadlines to deprecate today's algorithms by 2030 and disallow them by 2035, while the NSA's CNSA 2.0 requires quantum-resistant cryptography for new national-security acquisitions from 2027. **"Harvest now, decrypt later"** attacks mean the migration cannot wait for those deadlines to arrive: data captured today can be stored and broken the moment a cryptographically relevant quantum computer exists.

What turns this into an NHI problem is scale. Migrating a workforce to new algorithms is hard enough; migrating tens or hundreds of thousands of machine identities, each with its own keys and certificates, is impossible by hand. It demands exactly the infrastructure NHI governance requires anyway: a complete, automated, policy-driven view of every certificate and key across the estate, and the crypto-agility to swap an algorithm as a configuration change rather than a migration project. Building that capability now is what lets an organization keep pace with an attack surface that expands faster every quarter. The case for accelerating crypto-agility is no longer theoretical; it is the only way to be ready in time.

## 04 Why traditional IAM misses non-human identities

Most identity programs were designed for people, and they break down when applied to machines for a few structural reasons.

### 4.1 No owner, no lifecycle

Service accounts and keys are often created for a one-off task and never retired. Without an owner, no one rotates the credential, reviews its access, or decommissions it when the workload disappears, so it lingers as a standing risk.

### 4.2 Credentials, not sessions

Humans authenticate interactively and their sessions expire. NHIs rely on long-lived secrets and certificates that, once leaked, work until they are explicitly revoked, which requires knowing they exist in the first place.

### 4.3 Scale beyond manual reach

You can review a few thousand employees. You cannot manually review tens or hundreds of thousands of machine identities, each with its own credentials and renewal schedule.

### 4.4 Agents that act on their own

AI agents introduce runtime decision-making and tool-chaining that static access models never anticipated, and they can be manipulated through prompt injection. They need tighter, continuously evaluated controls, not a one-time grant.

## 05 Closing the blind spot: the CertiNext perspective

At CertiNext, we advocate treating non-human identities with the same rigor that mature programs already apply to people: discovery, ownership, least privilege, rotation, and retirement. Because the scale leaves no other option, that rigor has to be delivered through automation.

**CertiNext, powered by eMudhra,** brings certificate and machine-identity lifecycle management into a single control plane: automated discovery of certificates and keys wherever they live, policy-driven issuance and renewal across public and private CAs, and the crypto-agility to swap algorithms as post-quantum standards land. Combined with eMudhra's publicly trusted CA and SecurePass for privileged and workload access, it lets organizations govern the full spectrum of identity, human and non-human, rather than leaving machines in the dark.

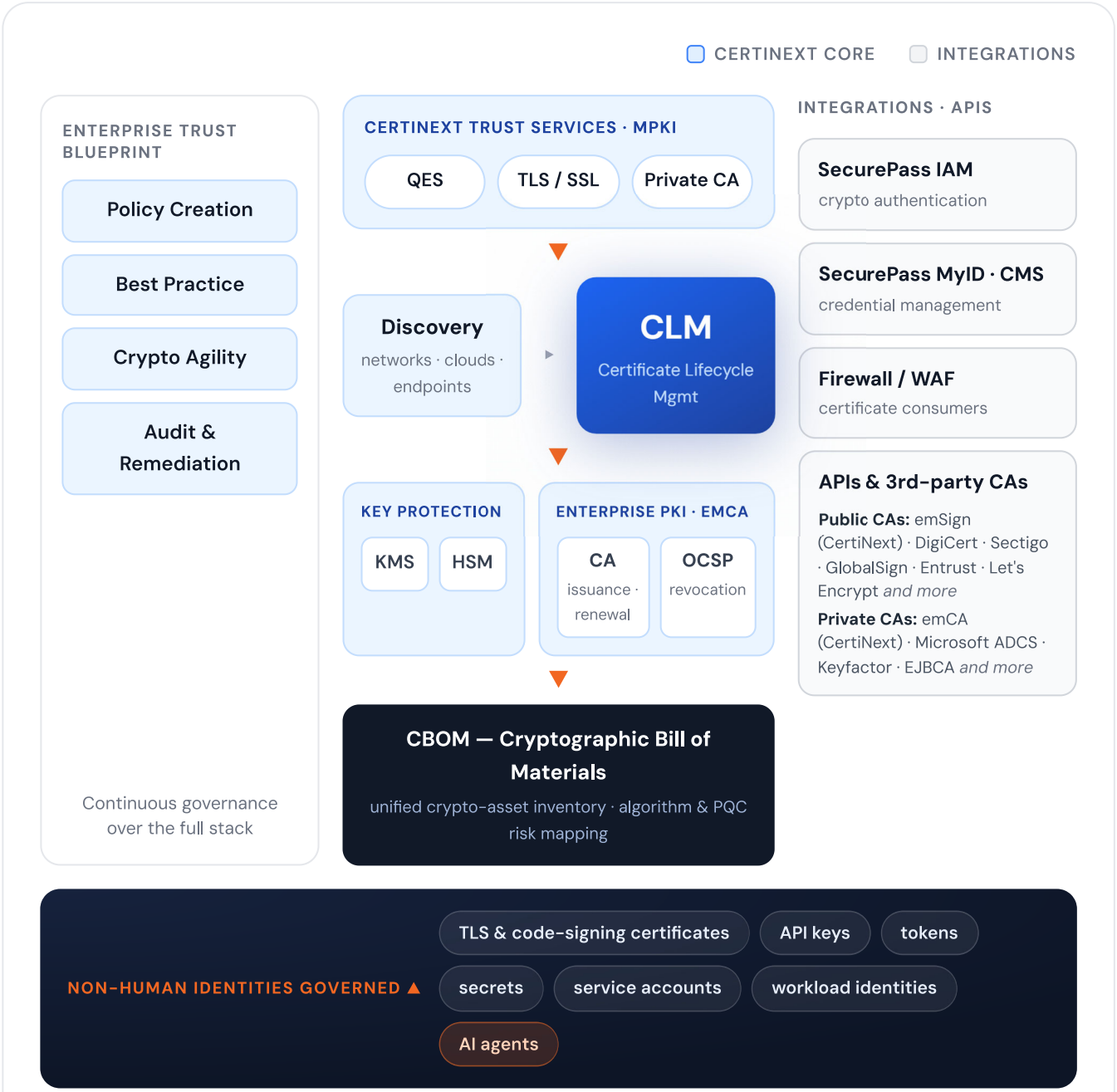
**Our guidance for teams starting now:**

- → **Make discovery continuous, not annual.** The estate changes by the minute; a point-in-time inventory is stale the moment it is finished.
- → **Automate the lifecycle end to end.** At NHI scale, issuance, renewal, and revocation have to run without human hands in the loop.
- → **Assign ownership to every non-human identity.** No identity should exist without an accountable owner and a defined expiry.
- → **Build for crypto-agility today.** Design so that changing an algorithm or CA is a configuration change, not a migration project.

FIGURE 1 · ARCHITECTURE

## The CertiNext Enterprise Trust Center

One control plane spanning discovery, issuance, key protection, and crypto-agility — governing every certificate and machine identity across the estate.




### From CLM to CPM, and beyond

Certificate Lifecycle Management → Certificate Posture Management

# 06 The NHI control checklist

A practical starting sequence for closing the blind spot in the next two quarters:

1. **Discover and inventory**
   Continuously discover every certificate, key, secret, service account, workload identity, and AI agent across cloud, on-premises, and CI/CD. You cannot govern what you cannot see.

2. **Assign ownership and expiry**
   Attach an accountable owner and a defined lifetime to every non-human identity. Flag and retire orphaned and unused identities.

3. **Enforce least privilege**
   Scope each NHI to the minimum access it needs, and review entitlements for machines as rigorously as for people — especially where agents can reach ERP, CRM, or financial systems.

4. **Automate rotation and renewal**
   Move to short-lived credentials and automated certificate renewal so that rotating a key across thousands of identities is a non-event, not a fire drill. Eliminate hard-coded secrets from code and pipelines.

5. **Govern AI agents explicitly**
   Apply runtime, continuously evaluated controls to agentic identities, with guardrails against prompt injection and clear boundaries on the tools and data they can invoke.

6. **Prepare for post-quantum**
   Build a cryptographic inventory now and adopt crypto-agility so ML-KEM and ML-DSA migration is a controlled rollout ahead of the 2030 and 2035 deadlines.

CONCLUSION

# Turn the blind spot into a source of trust.

Non-human identities are no longer an edge case. They are the majority of the identities running the modern enterprise, and the ones we govern least. The data shows the gap widening every year, agentic AI is accelerating it, and the post-quantum migration is removing any option to manage it by hand.

The organizations that treat this as an identity problem, not just a certificate problem, and that automate discovery, ownership, and lifecycle across every identity, will turn today's blind spot into a source of trust. That is the outcome **CertiNext, powered by eMudhra,** is built to enable: end-to-end trust for every identity, human and non-human.


## About CertiNext

CertiNext, powered by eMudhra, secures everything that matters: end-to-end trust for every identity, human and non-human. The platform unifies certificate lifecycle management, a publicly trusted certificate authority, and PQC-ready crypto-agility — so enterprises can discover, automate, and govern their entire identity estate from one control plane. Learn more at www.certinext.io.